The National Science Foundation
Office of Polar Programs
United States Antarctic Program

Information Resource Management Directive 5000.17
Non-USAP Systems

Organizational Function	Information Resource Management	Policy Number	5000.17
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Procedures	Effective Date	1 August 2004
		Review On	1 August 2006
Subject	Non-USAP Systems	Authorized By	Director, OPP
Office of Primary Responsibility	National Science Foundation Office of Polar Programs United States Antarctic Program	Responsible Official	Mr. Patrick D. Smith Technology Development Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	Phone	703.292.8032
		Fax	703.292.9080
		Web	www.nsf.gov/od/opp
Distribution	USAP-Wide	Status	Final Policy
Online Publication	www.polar.org/infosec/index.htm		

1. PURPOSE

Information systems which are not managed by NSF or its supporting contractors present a potential information security risk when connected to the USAP information infrastructure. This directive establishes policies to govern the connection of Non-USAP Information Systems to the USAP Information Infrastructure.

2. Background

USAP participants are normally provided with USAP-managed information resources to accomplish their mission. In some instances, participants need to connect non-USAP information systems to the USAP information infrastructure to accomplish their research or other mission activities. Users of non-USAP information systems must comply with all USAP policies while their systems are connected to the infrastructure. This policy identifies additional requirements for non-USAP systems that must be addressed before these systems may be connected to the infrastructure,or allowed to remain connected if an existing system.

3. GUIDING PRINCIPLES

The guiding principle of this policy is to minimize risk to the USAP infrastructure and the science and operations activities it supports.

- Non-USAP systems may be connected to the USAP information infrastructure only if they adhere to rules established to protect all users of the infrastructure.
- Non-USAP systems may be denied access at any time if they are deemed to be a hazard or burden to the to the USAP information infrastructure.

4. POLICY

Users of Non-USAP systems must comply with all USAP policies, standards and procedures while connected to the USAP infrastructure. Non-USAP systems themselves must conform to USAP intersystem connection specifications.

4.1 Definition of a Non-USAP System

An information system is considered a Non-USAP system when it can not be considered a USAP information system as defined in USAP Information Security Policy 5000.1, *The USAP Information Security Program*. This includes any information system or other type of system that supports USAP science or operations activities, but is not identified as an NSF system in NSF USAP property records, or is not managed by NSF or its USAP support contractors. This includes, but is not limited to, research systems and instruments procured by a grantee and intended for connection to the USAP infrastructure, personal computers, scientific and other types of instrumentation devices, servers, network devices, data recorders, wireless equipment, software applications, and other items.

4.2 Personal Information Devices

Personal systems intended for connection to NSF systems or the USAP infrastructure, such as a personal laptop or other computing device, are considered Non-USAP systems.

4.3 No Classified Information Processing

The USAP information infrastructure is not accredited for processing classified information, as defined by E.O 12968. Non-USAP systems that contain classified information will not be accommodated on the USAP information infrastructure. Users of Non-USAP systems shall not create, process, store, or disseminate classified information using the USAP information infrastructure at any time. Users of Non-USAP systems shall not connect any system used to process or store classified information to the USAP infrastructure, at any time.

4.4 Connection of Non-USAP systems to the USAP infrastructure

Owners of Non-USAP systems will ensure these systems comply with USAP information security policies, standards and procedures for infrastructure access prior to connecting the system to the USAP information infrastructure. Once connected, system owners will ensure the systems operate in a manner that complies with USAP rules of behavior and

system certification requirements. Failure to comply may result in the denial of infrastructure access privileges, up to and including removal from the infrastructure.

4.5 Certification of Non-USAP systems

USAP participants who deploy Non-USAP systems intended for connection to the USAP information infrastructure must provide detailed configuration information for these systems to the program information technology staff, prior to connecting the non-USAP system. This includes information systems, networks, data monitoring or recording devices, software applications or other devices. This information is to be provided as part of the Science Planning Process, and will be used to certify that the system complies with federal and NSF guidelines for the management of system vulnerabilities..

4.6 Connection Authorization

The USAP Information Security Manager (ISM) shall establish a process and procedures to review all Non-USAP systems that users intend to connect to the USAP infrastructure. The process shall include checks of hardware and software compatibility, as well as standard configurations of the operating systems to ensure compliance with the latest information security updates and protection components. No Non-USAP system may be connected to the infrastructure without authorization of the USAP ISM, or the OPP Technology Director. Authorization for system connection may be included in the Research Support Plan established during the Science Planning Process.

4.7 Protection against malicious applications, intrusion, and other forms of attack

To safeguard the USAP infrastructure, all Non-USAP information systems must implement appropriate measures to manage known vulnerabilities and protect against malicious applications, intrusions, and other forms of attack. Non-USAP systems shall use anti-virus software, where such software is commercially available, and other protective applications while connected to the USAP infrastructure. Where commercial protections are not available, OPP will consider requests to waive this provision.

4.8 Compliance with USAP standards

Owners of Non-USAP information systems are responsible for ensuring their systems meet USAP standards prior to the system's deployment. Any system found to be non-compliant will be refused connection to the infrastructure.

4.9 Network devices

Non-USAP network devices are prohibited unless specifically authorized by NSF. USAP participants must identify their need for non-USAP network devices.. Approved Non-USAP network devices must comply with all USAP policies, standards and procedures, and must be registered with the USAP ISM prior to connection to the infrastructure. For this policy, network devices include, but are not limited to, Iridium phones, radio modem devices, wireless access points, wireless network cards, routers, switches, firewalls, and software firewall applications.

4.10 Network monitoring tools

Non-USAP network monitoring tools are prohibited unless specifically authorized by NSF. USAP participants must identify their need for non-USAP network monitoring tools. Approved Non-USAP network monitoring tools must comply with all USAP policies, standards and procedures, and must be registered with the USAP prime contractor prior to connection to the infrastructure. For this policy, network monitoring tools include any software or hardware intended to monitor network traffic, including, but not limited to, sniffing tools, password recovery or cracking tools.

4.11 Waiver for Non-USAP Systems using unsupportable technology

USAP participants operating info systems that make use of unsupportable technology must apply for a waiver to this policy for their systems. The USAP ISM will establish a process to identify such non-USAP systems and evaluate the system to determine if a waiver is required. The NSF Head of Polar Research Support will approve or disapprove all waiver request for such systems based on the evaluation results. An analysis of systems employing older or unsupportable technologies, and their impact on the network will be included in the annual site assessments.

5. APPLICABILITY AND COMPLIANCE

This policy applies to all information resources, systems, and technology and to all users of these resources, systems and technology within the USAP operating environment or connected to the USAP information infrastructure. Compliance with this policy is as indicated in USAP Information Security Policy 5000.1, *The USAP Information Security Program*. Failure to comply with this policy will result in removal from the infrastructure, and may include additional sanctions as deemed appropriate by NSF.

6. RESPONSIBILITIES

Within the NSF and the USAP, several elements have responsibilities that relate to Non-USAP systems.

6.1 NSF Director of Polar Programs

The NSF Director of Polar Programs ensures uniform compliance with this policy in order to protect NSF USAP information systems. The Director of Polar Programs is the final authority to determine the level of acceptable risk associated with Non-USAP systems operations, while maintaining a cost-effective information security program.

6.2 NSF Head of Polar Research Support Section

The Head of Polar Research Support adjudicates requests for waivers to this policy.

6.3 USAP Information Security Manager

The USAP Information Security Manager (ISM) develops and implements a program to evaluate and certify Non-USAP systems for operation within the USAP.

6.4 Owners and Users of Non-USAP Systems

Owners and users of Non-USAP systems shall configure their systems to minimize known vulnerabilities, and to comply with federal information security requirements.

7. IMPLEMENTATION

The USAP ISM will develop appropriate policies, processes, standards, and procedures to ensure that Non-USAP systems are in compliance with USAP and NSF policy standards prior to their connection to the USAP information infrastructure. USAP organizational elements will publish procedures as appropriate to implement specific tasks needed to comply with this policy.

7.1 Non-USAP Systems

The USAP ISM will establish a program to evaluate the risks associated with connecting Non-USAP systems to the USAP infrastructure. The USAP ISM will publish guidelines to help ensure Non-USAP systems meet USAP standards for infrastructure connection.

7.2 Support to Non-USAP Systems

The USAP prime contractor may provide support to Non-USAP systems on a non-interference basis after all USAP mission requirements are satisfied, but is under no contractual obligation to do so, unless a Service Level Agreement or other formal tasking arrangement is established and approved by NSF OPP.

7.3 Requests for Waivers to this policy

Requests to waive provisions of this policy shall be submitted in writing to the Head of Polar Research Support, Office of Polar Programs. To ensure proper consideration of the waiver, requests must be submitted independent of any other documents submitted to OPP or the NSF, and may not be included in proposal documents such as the Operations Readiness Worksheet (ORW) or the Science Information Package (SIP).

7.4 Policy Review

The USAP Information Security Program Manager will review this policy in conjunction with major changes to the information infrastructure, as part of the USAP's participation in agency security audits, after each breach in system security, or every two years. The ISM will submit policy changes and new policies for review and approval by NSF OPP

8. AUTHORITY

Publication of this policy is in conformance with the authority of the National Science Foundation Act of 1950, as amended and extended, the Federal Information Security Management Act of 2002 and NSF Manual 7, The NSF Information Security Handbook.

KARL A. ERB
Director